[redacted]
June 12, 2025

The Honorable Stephanie A. Gallagher
United States District Judge
c/o Office of the Federal Public Defender
100 South Charles Street
Tower II, 9th Floor
Baltimore, Maryland 21201

Re: United States v. Mark Unkenholz
Criminal Case No. SAG-22-0105

Dear Judge Gallagher,

I have known Mr. Mark Unkenholz for over 25 years. I worked closely with him during many of those years. Mr. Unkenholz is best described as a patriotic American who worked hard to keep America safe. He was a technical leader serving in the National Security Agency's senior technical rank for over 20 years. I believe that Mr. Unkenholz is innocent of the charges against him. I believe that Mr. Unkenholz is caught up in the delicacy and complexity of the job that he had to the point where proving his innocence to a jury in a court of law would be extremely difficult.

The purpose of this paper is to show that Mr. Mark Unkenholz's emails that address technologies may very likely be addressing unclassified technologies of interest to the National Security Agency's Cybersecurity mission. This paper is solely based on unclassified information that was published by the Nationals Security Agency or in coordination with the National Security Agency.

The opinions in this paper are solely mine. While I am at a distinct disadvantage since I have only seen Mr. Unkenholz's unclassified redacted emails associated with the indictment and am relying on only unclassified information published by NSA or in coordination with NSA, I feel that my presentation is compelling.

Mr. Unkenholz worked for the National Security Agency (NSA) in an office that was "responsible for NSA's engagement with private industry".[1] NSA's website describes the Commercial Engagement Center (CEC) as working "with commercial companies to help make us safer at home and abroad. Today more than ever public-private partnerships are

[1] https://www.justice.gov/archives/opa/press-release/file/1489051/dl

needed to protect national security communications and to prevent foreign adversaries from harming our nation and our allies - both physically and in cyberspace."[2]

According to NSA's website, "NSA Cybersecurity prevents and eradicates threats to U.S. national security systems, with an initial focus on the Defense Industrial Base (DIB) and the improvement of the nation's weapons' security."[3] And, NSA "SIGINT plays a vital role in our national security by providing America's leaders with critical information they need to defend our country, save lives, and advance U.S. goals and alliances globally. ... At NSA, we must keep pace with advances in the high-speed, multifunctional technologies of today's information age. The ever-increasing volume, velocity and variety of current signals make the production of relevant and timely intelligence for military commanders and national policy-makers more challenging and exciting than ever. Modern telecommunications technology poses significant challenges to the SIGINT mission ...".[4]

From these statements, one can deduce that NSA Cybersecurity and NSA SIGINT will have interest in many of the same technologies but for different reasons.

From July 2014 through December 2022, NSA Cybersecurity (and its predecessor organization) has published or co-published 132 unclassified documents in the form advisories, info sheets, tech reports, and operational risk notices[5]. Many cybersecurity technologies were mentioned in these documents to include[6]:

- Quantum-resistant cryptography;
- Exposing critical vulnerabilities in widely used software and computer products;
- Exposing the threat and promote the understanding of Russian state-sponsored and cybercriminal tactics, techniques, and procedures;
- Exposing China's malicious activities, tactics, techniques, and procedures.

In 2014, two employees of NSA's Information Assurance Directorate published a paper that appeared in the 2015 48th Hawaii International Conference on System Sciences[7] that described the use of Private Information Retrieval (PIR) and other privacy preserving cryptographic techniques to protect information in unclassified networks.

NSA is active in several open national and international standards development organizations, for example, the InterNational Committee for Information Technology

[2] https://www.nsa.gov/business/programs/CEC/
[3] https://www.nsa.gov/Cybersecurity/Overview/
[4] https://www.nsa.gov/Signals-Intelligence/Overview/
[5] www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance
[6] https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/NSA%20Cybersecurity%20Year%20in%20Review%20v20221219.PDF, 2023.
[7] https://ieeexplore.ieee.org/document/7070089

Standards INCITS[8], ISO/IEC/SC 27/WG 2, Cryptography and security mechanisms, the Internet Engineering Task Force (IETF), National Institute for Standards and Technology (NIST) and The American National Standards Institute (ANSI)[9].

NSA is also an active contributor to software repositories on the internet such as GitHub, a web-based platform where software developers can store, share, and collaborate on code projects using a system called Git[10], and the Apache Software Foundation's Apache Incubator with the PIRK Project[11]. Pirk is a software framework for scalable Private Information Retrieval and is meant to provide a landing place for robust, scalable, and practical implementations of PIR algorithms. The initial scalable PIR algorithms and implementations of Pirk were developed at the National Security Agency[12].

The above is just a small sampling of the types of and the amount of unclassified information that NSA has openly published during the 2014-2022 timeframe.

Based on CEC's mission to protect national security communications and to prevent foreign adversaries from harming our nation and our allies, it seems that Mr. Unkenholz's emails may very well have been in the Cybersecurity context.

It has been several months since I have seen Mr. Unkenholz's redacted emails that were referenced in his indictment. I do recall several having a small number of consecutive words redacted. These seem to be a reference to a specific technologies. I do not recall any context around these words that would raise any doubt that they were not addressing any technology but cybersecurity technology. It seemed that whoever redacted these words may not have understood that they could have been used in the unclassified cybersecurity context since they may have seen the same technology referenced in classified SIGINT documents.

The classification issue seems to boil down to context – Cybersecurity or SIGINT. But is that the real issue?

As I understand the indictment, Mr. Unkenholz was charged with the communication and transmission of classified National Security Information (NDI) and willful retention of classified NDI, to summarize. Considering all of the publications that NSA Cybersecurity and its predecessor organization publicly issued, it is hard to believe that NSA's interest in technologies referenced in Mr. Unkenholz's emails was closely held. Furthermore, it is equally hard to believe that the information Mr. Unkenholz put into his emails could be used to the injury of the United States or to the advantage of any foreign nation. I wonder if

[8] See 2014 INCITS Technical Excellence Awards at https://www.incits.org/dotAsset/d94e6b1f-b066-4327-bc8a-8772eae87f59.htm

[9] https://www.nsa.gov/Cybersecurity/Partnership/Standards/

[10] https://github.com/orgs/nsacyber/repositories?type=all&page=2

[11] https://incubator.apache.org/projects/pirk.html

[12] https://cwiki.apache.org/confluence/display/incubator/PirkProposal

the Government asked the recipients of the emails to destroy them or remove them from their email system? Thus, it is likely that Mr. Unkenholz's emails that address technologies do not contain any National Defense Information.

While writing this, I realized the complexity of Mr. Unkenholz's situation in proving his innocence. The jury would have to have a good understanding of how NSA's CEC worked with companies. Mr. Unkenholz would have to present sufficient evidence to support his innocence for each of the 26 counts. If his attorneys were required to use the procedures in the Classified Information Protection Act, presenting convincing evidence could be challenging. I understand why Mr. Unkenholz chose to accept the plea bargain. But, I believe that felony conviction is much too harsh.

Respectfully,

John J Stasak, III

John J. Stasak, III